UK cyber security and critical national infrastructure protection

Stoddart, Kristan

Published in:
International Affairs

DOI:
10.1111/1468-2346.12706

Publication date:
2016

Citation for published version (APA):
Stoddart, K. (2016). UK cyber security and critical national infrastructure protection. *International Affairs*, *92*(5), 1079-1105. https://doi.org/10.1111/1468-2346.12706

UK cyber security and critical national infrastructure protection

KRISTAN STODDART*

David Cameron, then the British Prime Minister, stated in his foreword to the UK's 2015 Strategic Defence and Security Review (SDSR) that one of the priorities for Britain should be to 'remain a world leader in cyber security and ensure we have the capability to respond rapidly to crises as they emerge'.[1] This article analyses how the British government is handling the threats the UK is now facing at the high end of the cyber-security spectrum through potential attacks on UK critical national infrastructure (CNI).

The article will proceed in two stages. First, it will look at the public and private organisations and mechanisms that have been put in place to try to build cyber-resilience for CNI within the UK. Second, it will question whether these are sufficient to deal with the depth of the problems now facing the UK, and many other countries, in protecting their computer-controlled CNI assets. In doing so it will offer a series of recommendations to help increase CNI resilience, given that mainstream policy debates tend to subsume CNI vulnerabilities into much broader discussions of cyber security and cybercrime when CNI protection deserves considered and focused debate.[2]

Outlining the threats

Traditional forms of authority and power in the UK are vested in parliament, the judiciary, the police force and the military. Each is under challenge in cyberspace. The British government is largely unable to exercise sovereign control of

* This work is funded and supported by the SCADA-CSL programme of Airbus Group Endevr Wales, a joint research funding initiative of Airbus Group and the Welsh government. I wish to thank my partners on this project who have facilitated this programme of work and helped enormously with the research underpinning this article. They are: Dr Kevin Jones, who put together this project at Airbus Group Innovations; Hugh Soulsby, also of Airbus Group Innovations; Professor Andrew Blyth and Peter Eden of the University of South Wales; and Dr Peter Burnap and Dr Yulia Cherdantseva of Cardiff University. All are most valued colleagues on the SCADA Cyber Security Lifecycles Project that has funded and enabled this article and our related research. I also wish to thank the anonymous peer reviewers for this journal for helping make this a sharper and more comprehensive article, and Professor Andrew Dorman for his support as Commissioning Editor of *International Affairs*.

[1] HM Government, *National Security Strategy and Strategic Defence and Security Review 2015: a secure and prosperous United Kingdom*, Cm. 9161 (London, Nov. 2015), p. 6.

[2] Such as that found in the *International Journal of Critical Infrastructure Protection*, where computer scientists and engineers from academia and industry actively discuss these questions.

International Affairs **92**: 5 (2016) 000–000

UK cyberspace as it is unbounded by geographical constraints. The 2015 SDSR rightly highlighted that: 'The range of cyber actors threatening the UK has grown. The threat is increasingly asymmetric and global.'[3] There are few clear and unambiguous norms, rules and regulations in cyberspace, and the legal and governance frameworks currently in place are contested.[4] As noted above, this is not UK-specific but a global problem; the Deputy Director of the US National Security Agency (NSA), Richard Ledgett, publicly outlined these jurisdictional difficulties in an interview with the BBC in October 2015.[5]

Current cyber norms, rules and regulations are rooted at the national level and include laws governing what can or cannot be said or done on social media such as Twitter and Facebook. These have had to be updated or enacted as technology, and the take-up of that technology, evolve and, as they do so, change social, political and security dynamics. This is a fluid and dynamic environment and the law, whether national or supranational, is constantly playing catch-up with technology and what technology enables. Through this process of technological innovation and take-up:

> anyone with a laptop and a network connection can transmit information, whether 'one-to-one' or 'one-to-many', effectively globally and instantaneously in a variety of forms; process information … easily and cheaply with standard commercial software; and store information in vast quantities indefinitely on cheap, miniature and portable digital devices, or in the 'cloud', independent of any particular device.[6]

Within this rapidly evolving context it is clear that the British government at both national and regional levels is faced with a series of mounting difficulties in attempting to manage an ever-growing and deepening number of cybercrimes and cyber breaches, now seen every day in the UK and across the globe. The range of these is accelerating, promoted both by the expansion and low entry costs of computer technology and by the benefits this bestows and the malicious activities it enables in the ever-growing 'Internet of Things', which refers to the mass proliferation of sensors, devices and smart products, used to gather and transmit data over the Internet.

The actors behind these crimes and breaches are both foreign and domestic. They range from 'script kiddies'—(predominantly) young people engaging in illegal activities ranging from probing organizations to distributed denial of service attacks, either singly or through collectives such as the 'hacktivist' group 'Anonymous'—through to sophisticated hackers and crackers who could repre-

[3] HM Government, *National Security Strategy and Strategic Defence and Security Review 2015*, p. 19.

[4] See e.g. Paul Walker, 'Law of the horse to law of the submarine: the future of state behaviour in cyberspace', in M. Maybaum, A.-M. Osula and L. Lindström, eds, *2015 7th International Conference on Cyber Conflict: architectures in cyberspace* (Tallinn: NATO CCDCOE [Cooperative Cyber Defence Centre of Excellence] Publications, 2015), pp. 93–104.

[5] Gordon Corera, 'NSA warns of growing danger of cyber-attack by nation states', BBC News, 27 Oct. 2015, http://www.bbc.co.uk/news/world-us-canada-34641382. (Unless otherwise noted at point of citation, all URLs in this article were accessible on 15 July 2016.)

[6] David J. Betz and Tim Stevens, *Cyberspace and the state: towards a strategy for cyber-power* (Abingdon: Routledge/International Institute for Strategic Studies, 2011), p. 112. See also Martin C. Libicki, *Conquest in cyberspace: national security and information warfare* (New York: Cambridge University Press, 2007).

sent Advanced Persistent Threats (APTs) to a nation-state. This poses a number of difficulties for the UK, and other nations that uphold the rule of law, which is 'concerned with the organization of public authority within states and the ability to make policy and to regulate behaviour effectively … [entailing] both authority and control'.[7]

The exercise of such authority and control is problematic given that the internet has no geographical borders and domestic state intrusion is widely resisted (as evidenced in the wake of the PRISM mass surveillance programme and polarizing views of the whistleblower and ex-NSA contractor Edward Snowden). The internet can be policed only weakly, owing to the sheer volume of traffic (Big Data and associated metadata), and a series of political, social and legal issues surrounding norms and jurisdictions. As Jamie Bartlett notes in his book on the hidden 'dark net', 'the battle for ideas, influence and impact is moving online' (and is particularly active among extremist groups).[8]

Placing these observations in a wider context, Betz and Stevens argue that in terms of 'cyber war', 'Perhaps the most persistent concern … is the idea that it [the cyber realm] deepens asymmetries of power between strong states and weaker states, and between all states and some "super-empowered" non-state actors … as David proved against Goliath, strength can be beaten.'[9] Such 'David and Goliath' metaphors draw their basis from the huge extent of reliance upon computer technology in developed states. This dependence, and the concomitant vulnerability to cyber attack, is at its most potent in relation to Industrial Control Systems (ICS)—particularly SCADA (Supervisory Control and Data Acquisition) systems. They are a deeply embedded and longstanding technology in the UK and many other developed states, dating back to the 1940s. Many SCADA systems have been in place since the 1980s and 1990s, when the internet was in its infancy and computer security not an acute consideration. Today, the situation is very different. Attacks on these computer-controlled industrial systems could cause electricity blackouts and water shortages, or disrupt financial services. Now there are publicly discussed fears of a 'cyber Pearl Harbor', a 'cyber 9/11' or even a state-wide 'Cybergeddon' attack, aimed at crippling or seriously damaging a nation, which could cascade to other states through attacks on CNI.[10]

The UK's national infrastructure is defined by the government as:

> those facilities, systems, sites and networks [physical and electronic] necessary for the functioning of the country and the delivery of the essential services upon which daily life in the UK depends … There are certain 'critical' elements of national infrastructure that if lost would lead to severe economic or social consequences or to loss of life in the UK. These critical elements make up the critical national infrastructure (CNI).[11]

[7] Betz and Stevens, *Cyberspace and the state*, p. 57.
[8] Jamie Bartlett, *The Dark Net: inside the digital underworld* (London: Heinemann, 2014), p. 49.
[9] Betz and Stevens, *Cyberspace and the state*, p. 90.
[10] See e.g. Richard A. Clarke and Robert K. Knake, *Cyber war: the next threat to national security and what to do about it* (London: ECCO, 2010); Elisabeth B. Miller and Thom Shanker, 'Panetta warns of dire threat of cyberattack on US', *New York Times*, 11 Oct. 2012, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&_r=0.
[11] This definition is 'broadly similar' to that of the EU. See Cabinet Office, *Strategic framework and policy statement*

International Affairs 92: 5, 2016

The potential for disruption or damage of CNI was recognized by the 2015 SDSR, which reasserted cyber attacks as a Tier One threat to national security. It warned that:

> Growing numbers of states, with state-level resources, are developing advanced capabilities which are potentially deployable in conflicts, including against CNI and government institutions. And non-state actors, including terrorists and cyber criminals can use easily available cyber tools and technology for destructive purposes.[12]

UK central government organizations and responsibilities

UK central government departments and agencies, including the Ministry of Defence (MoD), work with other governments across a range of common issues. For the MoD these channels of collaboration include the Foreign and Commonwealth Office's (FCO's) International Cyber Policy Unit and NATO;[13] at the European level they include the European Network and Information Security Agency (ENISA).[14]

Domestically there is little direct 'governance' of CNI in the UK comparable to the way nationalized industries were run centrally by government prior to their privatization during the 1980s and 1990s. Instead, as CNI is largely owned and operated by private industry, its governance resembles more a form of macro-management in terms of oversight and regulation, similar to the way the National Health Service and National Rail are now run. Micro-management in the nine sectors that comprise CNI (communications, emergency services, energy, financial services, food, government, health, transport, water), each of which constitutes a large and complex set of organizations with enormous budgets, is undertaken through regulation and oversight via formal and informal statutory regulators and legal bodies. This is in line with neo-liberal practices that promote minimum state intervention.

Activities to combat threats to SCADA and other ICS embedded across industries are currently overseen in the UK by a national Computer Emergency Response Team (CERT-UK) established in 2014, along with the Government Computer Emergency Response Team, whose task is to provide warnings, alerts and assistance to public-sector organizations. CERT-UK is one of many such bodies that have been set up by national governments. It is designed to 'work closely with industry, government and academia to enhance UK cyber resilience'.[15] Another initiative was the formation of the Cyber Security Information Sharing Partner-

on improving the resilience of critical infrastructure to disruption from natural hazards (London, March 2010), p. 8, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62504/strategic-framework.pdf.

[12] HM Government, *National Security Strategy and Strategic Defence and Security Review 2015*, p. 19.

[13] MoD, *Cyber primer* (Swindon, Dec. 2013), pp. 1-19–1-20, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/360973/20140716_DCDC_Cyber_Primer_Internet_Secured.pdf.

[14] Pinsent Masons, 'EU lacks "unified vision" for "important" standards on cyber security, says ENISA', *Out-Law.com*, 30 March 2105, http://www.out-law.com/en/articles/2015/march/eu-lacks-unified-vision-for-important-standards-on-cyber-security-says-enisa/.

[15] https://www.cert.gov.uk/.

ship (CiSP), which by 2014 had a membership of 750 organizations.[16] CiSP is described in the following terms:

> CiSP is now a part of CERT-UK. CiSP was launched in March 2013 and is a joint, collaborative initiative between industry and government to share cyber threat and vulnerability information in order to increase overall situational awareness of the cyber threat and therefore reduce the impact upon UK business … CERT-UK will be able to add the day to day experience of working with critical national infrastructure companies in handling the incidents they face alongside the international dimension.[17]

In addition, the CiSP forums (which were established in the run-up to the 2014 Commonwealth Games in Glasgow and that year's NATO summit in Newport, Wales) are intended to become 'permanent hosts for such information sharing in Scotland and Wales'.[18] These programmes of work and education were augmented in June 2014 with the launch of 'Cyber Essentials', which is intended to be

> a major new Government-backed and industry supported scheme to incentivise widespread adoption of basic security controls that will help to protect organizations against the commonest kind of internet attacks. The scheme is constructed to be affordable and practical for all firms, small as well as large. Certification comes with a badge which firms can use to help demonstrate their security credentials to customers and investors, and which insurers can take into account when considering firms for relevant insurance policies.[19]

It is run by the Government Communications Headquarters (GCHQ), the Department for Business, Innovation and Skills (BIS)[20] and the Cabinet Office, and also seeks to improve cyber-security risk management and companies' ability to take out insurance against cyber attacks.[21]

In the attempt to keep up to date with the multiplying cyber threats Britain faces, CERT-UK works with a number of other agencies—some public sector and some private. Also, working with Britain's allies (particularly the United States) to combat cross-border threats, it 'oversees a programme of exercises to support critical sectors in preparing for the potential impact of a destructive cyber attack', including through the Heartbleed and Shellshock vulnerabilities.[22]

Activities to combat serious crime are undertaken by the National Crime Agency (NCA), established in October 2013, which now incorporates legacy organizations including the National Cyber Crime Unit (NCCU), the Police e-Crime Unit and the Serious Organized Crime Agency (SOCA).[23] The NCCU

[16] Cabinet Office, *The UK Cyber Security Strategy: report on progress and forward plans December 2014* (London, Dec. 2015), p. 5, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___.pdf.
[17] Cabinet Office, *The UK Cyber Security Strategy*, p. 5.
[18] Cabinet Office, *The UK Cyber Security Strategy*, pp. 5–6.
[19] Cabinet Office, *The UK Cyber Security Strategy*, p. 7.
[20] This is now likely to be taken up by the Department for Business, Energy & Industrial Strategy (BEIS) which was created in July 2016.
[21] 'HMIC report highlights concern over cybercrime plans', BBC News, 10 April 2014, http://www.bbc.co.uk/news/uk-26963938.
[22] Cabinet Office, *The UK Cyber Security Strategy*, pp. 13–14.
[23] MI5, 'What we do', https://www.mi5.gov.uk/home/about-us/what-we-do/major-areas-of-work.html. See

'brought together specialists from the Police Central e-Crime Unit in the Metropolitan Police Service and SOCA Cyber to create expert technical, tactical intelligence and investigation teams'.[24] These bodies work with GCHQ 'to develop the skills and technology required to combat elite cyber crime threats to the UK'.[25]

There are also nine Regional Organized Crime Units (ROCUs), each of which has a dedicated cybercrime unit. This also includes Operation Falcon (Fraud and Linked Crime Online) within the Metropolitan Police—the largest of the UK's 48 police forces and the lead force for cybercrime.[26] The remit of Falcon, a joint operation by the Fraud Squad and the Met's cybercrime unit, is 'to disrupt and arrest cyber criminals attacking London businesses'.[27] In addition the NCCU has augmented its activities overseas to work with Europol, US agencies and Interpol to understand the global cybercrime threat, coordinate activity against priority threats and develop relationships with international partners to support cooperation on prosecutions, including posting officers overseas.[28]

With the vast majority of cybercrime emanating from abroad, more needs to be done, including through the 'Cyber Streetwise' public awareness campaign.[29] The availability of inexpensive software, and of online evasion software and tactics on the internet, makes it difficult for the police to track and trace cybercrime, and they have to assess whether they are able to pour scarce resources into difficult prosecutions.[30] The use of The Onion Router (TOR) and proxy servers only compounds the problems facing the police and intelligence agencies in terms of identification/attribution and prosecution, as does the growing use of encryption by major technology companies.[31] As the police might well be tasked as one of the 'first responders' to any industrial emergency, their role is important, but they are under-resourced and they do not appear to have received any new money from the SDSR.[32] This deficiency needs to be addressed.

The UK government tasked the ROCUs with sharing cyber-security information regionally to assist local businesses to protect themselves from cybercrime. This information-sharing operation, carried out in conjunction with CERT-UK,

---

also NCA, 'Working in partnership', http://www.nationalcrimeagency.gov.uk/about-us/working-in-partnership.

[24] NCA, 'National Cyber Crime Unit', http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit.

[25] HM Government, *2010 to 2015 government policy: cyber security*, policy paper (London, updated May 2015), appendix 1, 'Setting up a National Cyber Crime Unit', https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace/supporting-pages/setting-up-a-national-cyber-crime-unit.

[26] 45 of these cover geographical regions and three are special police forces like the British Transport Police.

[27] HM Government, *2010 to 2015 government policy: cyber security*, appendix 1, 'Setting up a National Cyber Crime Unit'.

[28] Cabinet Office, *The UK Cyber Security Strategy*, pp. 11, 16–18.

[29] HM Government, 'New campaign urges people to be "Cyber Streetwise"', https://www.gov.uk/government/news/new-campaign-urges-people-to-be-cyber-streetwise; https://www.cyberstreetwise.com/.

[30] Views expressed under the Chatham House rule at the conference 'Enhancing the UK's cyber resilience: working in partnership to reduce cyber risk in the digital age', London, 24 March 2015.

[31] See e.g. Joe Miller, 'Google and Apple to introduce default encryption', BBC News, 19 Sept. 2014, http://www.bbc.co.uk/news/technology-29276955; 'Tor Project makes efforts to debug dark web', BBC News, 23 July 2014, http://www.bbc.co.uk/news/technology-28447023.

[32] Derek du Preez, 'London Police Commissioner's cyber-crime open letter laughed at by industry', *Computerworld UK*, 13 Aug. 2013, http://www.computerworlduk.com/security/london-police-commissioners-cyber-crime-open-letter-laughed-at-by-industry-3463524/.

began in the east Midlands and south-east of England in August 2014 as part of CiSP. The global context for these efforts is illustrated by Verizon's 2014 Data Breach Report demonstrating the wide range of sectors and businesses being attacked and how they are being attacked.[33] Notwithstanding the policies set out in the 2015 SDSR, which will require time to mature, current government and police action has not stopped UK organizations and UK-based companies from being hacked.

Among organizations attacked in this way are internet service providers: for example, in October 2015 TalkTalk's unencrypted customer data, including addresses and banking details, were compromised with simultaneous financial reputational damage, including an immediate 10 per cent dip in share value. These hacks produce a wider loss of confidence in business dealings over the internet and exact unwelcome costs to business in insuring against malicious cyber breaches and the range of threats and risks. It is perhaps no surprise that business leaders are calling on the government to do more while recognizing that this is mainly a corporate responsibility. With the 2015 SDSR making clear that the government will seek to help companies secure their data, it remains to be seen what further breaches will occur and where blame will be directed.

The Institute of Directors has pointed out that 'only "serious breaches" made the headlines, but attacks on British businesses "happen constantly"',[34] while the City of London Police Commissioner has stated publicly that 80 per cent of cybercrime goes unreported and 'cyber-crime could become bigger than the drugs trade'.[35] Cyber attacks already grab headlines and public attention; an attack on public utilities or financial services could have far more profound social, financial and political consequences than any cybercrime yet reported. This is already recognized by the EU, which is finalizing the Directive on Security of Network and Information Systems (NIS Directive): this requires CNI owner–operators 'to adopt risk management practices and report major incidents to the national authorities'.[36]

Against this background, the UK's 2009 'Cyber Security Strategy' led to the formation of the multi-agency Cyber Security Operations Centre (CSOC) hosted by GCHQ, operating alongside the Communications Electronics Security Group (CESG).[37] CSOC is intended to 'actively monitor the health of cyber space and co-ordinate incident response; enable better understanding of attacks against UK

[33] Verizon Data Breach Investigations Report 2014, 26 July 2016, http://www.nu.nl/files/Verizon.pdf. These findings were reconfirmed in Verizon's Data Breach Investigations Report 2016, 26 July 2016, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/.

[34] 'TalkTalk attack: "urgent action needed" on cyber-crime', BBC News, 24 Oct. 2015, http://www.bbc.co.uk/news/uk-34622754.

[35] Doug Drinkwater, 'London police chief admits cyber-crime failings', *SC Magazine*, 15 April 2015, http://www.scmagazineuk.com/london-police-chief-admits-cyber-crime-failings/article/409167/.

[36] The adoption of this piece of legislation is now doubtful following the June 2016 Brexit referendum (Brexit). On the directive, see 'The Directive on security of network and information systems (NIS Directive)', 16 March 2015, https://ec.europa.eu/digital-agenda/en/news/network-and-information-security-nis-directive.

[37] This group is still known as CESG, despite the somewhat outdated title, and dates back to 1919. See 'CESG: the Information Security Arm of GCHQ', https://www.cesg.gov.uk/articles/cesg-information-security-arm-gchq, accessed 14 July 2015.

networks and users; [and] provide better advice and information about the risks to business and the public'.[38] It is designed:

> to monitor developments in cyber space (ultimately providing collective situational awareness), analyse trends, and to improve technical response coordination to cyber incidents … [for] a better understanding of cyber security risks and opportunities, it will also help to ensure coherent dissemination of information across government, industry, international partners, and the public … [drawing] from across government and key stakeholders.[39]

It is directed by the Office of Cyber Security and Information Assurance (OCSIA), which in 2010 replaced the Office of Cyber Security (itself only established in 2009) and works with government agencies and departments including the Home Office, MoD, GCHQ, CESG (which is housed within GCHQ), the Centre for the Protection of National Infrastructure (CPNI), FCO and BIS/BEIS. OCSIA is designed to advise the cabinet and National Security Council (NSC) by providing strategic direction and coordination for government in the field of cyber security and information assurance.[40]

In essence OCSIA's remit is to try to 'secure' the UK's cyberspace.[41] This follows a line of reasoning presented by Betz and Stevens who, in *Cyberspace and the state*, argue that cybercrime and hacking represent 'a significant challenge to states whose sovereignty and data security are in a state of constant skirmish with cyberspace challengers, whether they be state, non-state or quasi-state'.[42] OCSIA built on the UK's 2011 National Cyber Security Strategy, which had four main objectives:

> 1) The UK to tackle cyber crime and be one of the most secure places in the world to do business in cyberspace
>
> 2) The UK to be more resilient to cyber attacks and better able to protect our interests in cyberspace
>
> 3) The UK to have helped share an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies
>
> 4) The UK to have the cross-cutting knowledge, skills and capability it needs to underpin all our cyber security objectives.[43]

The last of these objectives was part of a national education programme begun by the Cabinet Office and GCHQ through the National Cyber Security Programme

[38] Cabinet Office, *Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space* (London, June 2009), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf.

[39] Cabinet Office, *Cyber Security Strategy of the United Kingdom*.

[40] HM Government, 'Office of Cyber Security and Information Assurance', https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance.

[41] Shaun Harvey, 'Unglamorous awakenings: how the UK developed its approach to cyber', in Jason Healey, ed., *A fierce domain: conflict in cyberspace 1986–2002* (Vienna, VA: Cyber Conflict Studies Association/Atlantic Council, 2013), pp. 261–2.

[42] Betz and Stevens, *Cyberspace and the state*, p. 34. See also remarks at the launch of the book in Washington DC, 1 Feb. 2012, https://www.youtube.com/watch?v=NeA3r_s5zCs.

[43] https://www.cert.gov.uk/; see also Thomas Rid, *Cyber war will not take place* (London: Hurst, 2013), p. 112.

(NCSP).[44] The NCSP began in 2011 (and continues to date), with funding of £860 million through to 2016, although the overall figure spent on cyber security is higher.[45] This £860 million was more than doubled in the 2015 SDSR, and the £1.9 billion earmarked for cyber security from 2016 to 2020 heralds the second five-year National Cyber Security Strategy and NCSP planned to be launched in October 2016.[46] It includes funding for offensive cyber capabilities through the National Offensive Cyber Programme run jointly by the MoD and GCHQ and for strengthened computer networks within government. The SDSR also makes it clear that the government intends to be more open in sharing information on cyber threats, ranging from 'lone wolves' to APTs, in partnership with the private sector. Some information will also be shared with NATO and allied nations.[47]

Importantly, given the large number of organizations (a number of which are relatively recent creations) dealing with cyber security, the SDSR also announced the establishment of a new National Cyber Security Centre (NCSC). This is to be based in London but under the leadership of GCHQ. The NCSC is designed to 'manage our future operational response to cyber incidents, ensuring that we can protect the UK against serious attacks and minimise their impact'.[48] It is intended that the NCSC 'will be the bridge between industry and government, simplifying the current complex structures, providing a unified source of advice and support, including on managing incidents. It will be a single point of contact for the private and public sectors alike' and will run CiSP.[49] As the then Chancellor George Osborne recognized, 'we need to address the alphabet soup of agencies involved in protecting Britain in cyberspace'.[50]

Despite ambitions for the NCSC, GCHQ continues to claim the majority of cyber-security funding to 'provide protection at pace and scale to key networks of national significance'. It will share intelligence on state-level threats and serious crime through cleared communications service providers to enable early warning to be given and action to be taken. While the 2015 SDSR suggests that this information-sharing will now be more forthcoming than formerly,[51] much of GCHQ's work to protect Britain's CNI from cyber attack remains classified, with government oversight provided through the parliamentary Intelligence and Security Committee.

[44] HM Government, 'New pathways for the UK's future cyber security experts', press release, 9 March 2015, https://www.gov.uk/government/news/new-pathways-for-the-uks-future-cyber-security-experts.

[45] Francis Maude, 'Written statement to parliament. UK Cyber Security Strategy: statement on progress 3 years on', 11 Dec. 2014, https://www.gov.uk/government/speeches/uk-cyber-security-strategy-statement-on-progress-3-years-on; National Audit Office, *The UK cyber security strategy: landscape review* (London, Feb. 2013), http://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf.

[46] 'New National Cyber Security Centre set to bring UK expertise together', https://www.gov.uk/government/news/new-national-cyber-security-centre-set-to-bring-uk-expertise-together, accessed 9 June 2016.

[47] HM Government, *National Security Strategy and Strategic Defence and Security Review 2015*, pp. 40–41.

[48] HM Government, *National Security Strategy and Strategic Defence and Security Review 2015*, p. 41.

[49] *Prospectus introducing the National Cyber Security Centre*, 2016, pp. 2 and 8. Available from https://www.gov.uk/government/publications/national-cyber-security-centre-prospectus.

[50] 'Chancellor's speech to GCHQ on cyber security', 17 Nov. 2015, https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security.

[51] Cabinet Office, *The UK Cyber Security Strategy*, p. 13; HM Government, *National Security Strategy and Strategic Defence and Security Review 2015*, pp. 40–41, 73.

In addition, a Centre for Cyber Assessment (CCA) was established at GCHQ in April 2013. The CCA, whose membership is drawn from across government departments, agencies and law enforcement bodies, is the cyber equivalent of the Joint Terrorism Analysis Centre (JTAC).[52] It is funded from the NCSP and is designed to provide all-source intelligence-driven reports to government customers including 'top industry bodies and companies as part of our wider work to protect British national security, our citizens and businesses'.[53] These dialogues with industry are intended to represent a partnership between government, regulators and industry.[54]

The government has promulgated a list of '10 Steps to Cyber Security' as part of this programme in an attempt to improve business awareness of cyber risks.[55] Other initiatives include a cyber 'health check' for FTSE350 companies and guidance from BIS for the financial services sector and for non-executive directors. In addition BIS has hitherto published an annual Information Security Breaches Survey, 'to assess the level of information security breaches affecting UK businesses and raise awareness of the need for industry to take action'. This survey found that 81 per cent of large organizations and 60 per cent of small organizations reported at least one breach during 2014. These percentages were down from 2013, but the scale of attacks in terms of cost and severity was higher, with average losses of £65,000–£115,000 reported for small organizations and between £600,000 and £1.15 million for large organizations. Over two-thirds (69 per cent) of company boards now actively assess their cyber-security vulnerabilities, up from 44 per cent in July 2013.[56] 'Cyber' has long been considered the business of 'IT departments', which are simply tasked to 'get on with it' with minimal board-level involvement. On the contrary, shared cyber security best practices need to be embedded in the same way that industrial and workplace safety and security are part of business culture, not an afterthought.

GCHQ also certifies companies working in cyber incident response, providing guidance on a 'bring your own device' security policy which allows people to use their personal computer devices at work, and engages with industry to try to ensure companies have cyber-security products able to defend against cyber attack. It does the latter through commercial product assurance, which includes publishing a set of security characteristics for domestic equipment required for the UK's smart metering programme. GCHQ also works with private industry to conduct unclassified research, experimentation and code development.[57]

[52] On the JTAC, see below.

[53] The existence of the CCA was made public in June 2015, specifically to encourage these dialogues and partnerships. See 'Foreign Secretary highlights the work of the Centre for Cyber Assessment', https://www.gchq.gov.uk/news-article/foreign-secretary-highlights-work-centre-cyber-assessment, accessed 29 Dec. 2015.

[54] 'Communiqué from the "Strengthening the cyber security of our essential services" event', 5 Feb. 2014, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/284085/Communique_-_Strengthening_the_Cyber_Security_of_Our_Essential_Services.pdf.

[55] https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary.

[56] Cabinet Office, *The UK Cyber Security Strategy*, p. 5.

[57] Cabinet Office, *The UK Cyber Security Strategy*, pp. 5, 9–10.

CPNI, meanwhile, works in close collaboration with key partners including CESG and the police, including specialist organizations within the police such as the National Counter Terrorism Security Office (NaCTSO), located within the same building as CPNI, and the countrywide Counter Terrorism Security Advisor (CTSA) network. CPNI states that: 'Government departments have lead responsibility for ensuring appropriate steps are taken within their sectors to improve protective security. They also lead on the identification of critical infrastructure within their sectors in consultation with CPNI and sector organizations.'[58] CPNI identifies the following government departments as having lead responsibility in the nine key sectors identified above:

- communications—Department for Business, Innovation and Skills;
- emergency services:
  - Ambulance—Department of Health;
  - Fire—Department for Communities and Local Government;
  - Maritime and Coastguard Agency—Department for Transport;
  - Police—Home Office;
- energy—Department for Energy and Climate Change;
- finance—HM Treasury;
- food—Department for the Environment, Food and Rural Affairs and Food Standards Agency;
- government—Cabinet Office;
- health—Department of Health;
- transport—Department for Transport;
- water—Department for the Environment, Food and Rural Affairs.

Despite these overarching roles, organizations and policies, cyber attacks continue to grow both quantitatively and qualitatively. In terms of CNI vulnerabilities, Misha Glenny notes:

> Cyber weapons are the hacking tools … to penetrate the computer systems of an enemy's CNI … such as their energy and water grids. Once in control of the system … the cyber commander can order their shutdown (or, as we know from Stuxnet, trigger a very damaging explosion[59]) so that in a matter of days the affected society will be reduced to Stone-Age technology.[60]

Stuxnet was the vehicle for the most widely known, and most widely reported, attack to date on a SCADA system. Stuxnet adversely affected the centrifuges in the Natanz nuclear processing plant in Iran, unbeknown to the operators. The software might have been installed in the plant via a USB device rather than through external infection, although later it did 'escape' onto the internet, where it can be further refined beyond the original intent of its programmers (widely suspected

[58] CPNI, 'Who we work with', http://www.cpni.gov.uk/about/Who-we-work-with/.

[59] Although Stuxnet did not cause an explosion it demonstrated a proof of concept that alterations made by computer code can have physical impacts. This can include explosions, for example by turning off safety features in ICS, including alerts for the operators that something is wrong.

[60] Misha Glenny, *Dark market: how hackers became the new Mafia* (London: Vintage, 2012), p. 245.

to be elements of the Israeli and US intelligence agencies).[61] A less widely known but disturbing attack was made on the SCADA systems of a German steel mill in 2014, causing the blast furnace to shut down with massive damage but no loss of life.[62] States can lose control of the coding capabilities of the next generation of Stuxnets, which will have the potential to act on a much greater scale, and this poses a proliferation problem.[63]

In view of the burgeoning threats and potential perpetrators, the current patchwork quilt of responsibilities and government organizations needs to be coordinated through a dedicated and strengthened single body. The 2015 SDSR appears to intend the NCSC to be this focal point for CNI protection and for 'cyber incidents' more generally. But what now happens to OCSIA and CPNI and the other government organizations with a stake in cyber security? While the creation of a central hub for UK cyber security is to be welcomed, as is the then Chancellor George Osborne's declared intent (as chair of the cyber subcommittee of the NSC) to make a 'top priority of cyber security', it is important to get this right.[64] The National Cyber Security Centre could significantly improve macro-level tactical and strategic oversight, but still the risk remains that there are simply too many organizations dealing with many common issues.

The Royal United Services Institute has also expressed concern that cyber security in the UK is being dominated by GCHQ. Although there will be 'representation from a broad range of stakeholders' at the NCSC, under the new structure 'almost the entire focus of the UK approach to cyber-security [will be] located in GCHQ'. RUSI legitimately questions 'whether this is entirely helpful' and calls for 'further debate' on the point.[65] Although much is yet to be resolved ahead of the 2016 National Cyber Security Strategy, this debate should focus on where to recruit new blood across a wide spectrum encompassing both technical and policy worlds, and where to draw from existing expertise, found not only within GCHQ, but also in OCSIA, CPNI and other relevant bodies, as well as industry.

It is commendable that the NCSC is intended to be staffed by 'series of teams, expert in the cyber security of their own sectors, from banking to aviation, but able to draw on the deep expertise here [GCHQ], and advise companies, regulators, and government departments'.[66] Nevertheless, it is worthwhile considering whether GCHQ is set to become too powerful in the field of cyber security at the expense of other agencies and other bodies, such as the police—especially

[61] For an excellent synopsis of Stuxnet, see Ralph Langer, 'Stuxnet's secret twin', *Foreign Policy*, 19 Nov. 2013. See also Kim Zetter, *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon* (New York: Crown Business, 2014).

[62] 'Hack attack causes "massive damage" at steel works', BBC News, 22 Dec. 2014, http://www.bbc.co.uk/news/technology-30575104.

[63] Views expressed under the Chatham House rule at CyCon 2015, Tallinn, Estonia, 26–29 May 2015.

[64] HM Government, 'Chancellor sets out vision to protect Britain against cyber threat in GCHQ speech', 17 Nov. 2015, https://www.gov.uk/government/news/chancellor-sets-out-vision-to-protect-britain-against-cyber-threat-in-gchq-speech.

[65] Evan Lawson, 'The Joint Forces Command and the 2015 SDSR: too soon to tell', Royal United Services Institute, 27 Nov. 2015, https://rusi.org/commentary/joint-forces-command-and-2015-sdsr-too-soon-tell.

[66] 'Chancellor's speech to GCHQ on cyber security'.

when the police, and many government departments, have seen their budgets cut through financial austerity and spending reviews.

CPNI already works closely with OCSIA and CSOC as well as the Civil Contingencies Secretariat in the Cabinet Office, 'which works to enhance the UK's ability to prepare for, respond to and recover from emergencies'.[67] Significantly, CPNI also maintains 'close relationships with organizations and businesses that own or operate the national infrastructure. Relationships have been built up over many years between our experienced security advisers and security managers in the sectors.'[68] On the hardware front, CPNI 'assures a wide range of physical security products developed by manufacturers for use on critical national infrastructure (CNI) sites … [and] works with a range of external partners on the development of professional standards'.[69] Domestically, cyber risk is built into departmental risk management as part of each department's audited Statement of Internal Control.[70] Cyber risk reviews for companies operating CNI have also been adopted.[71]

At the global level, CPNI has a 'close relationship with many international partners, including overseas Governments, agencies and businesses'. This includes contributing to Overseas Business Risk, a joint endeavour run by the FCO, UK Trade and Investment and BIS, providing UK business with information relating to 'security related risks companies face when operating overseas'.[72]

The British government also has responsibilities to its partners in NATO and, until the UK negotiates withdrawal following the 2016 Brexit referendum, the EU that are described in the MoD's *Cyber primer* document as complex—'a complexity aggravated by the need to include national organizations, such as computer emergency response teams (CERTs), and national and international legal requirements'.[73] This complexity embraces:

> a) The NATO Communications and Information (NCI) Agency [which] manages those networks actually owned by NATO. Formed on 1 July 2012 … the NCI Agency also has a coordinating role across individual NATO and NATO-nation CERTs.
>
> b) Cooperative Cyber Defence Centre of Excellence [CCDCOE]. Their mission is to enhance capability, cooperation and information sharing across NATO, and its nations and partners in cyber defence through education, research & development, lessons-learned and consultation.
>
> c) ENISA. This agency is the European Union focus for technical assistance for the security aspects of cyberspace.[74]

This tier of international institutions operates alongside national cyber command structures, a number of which are engaged in liaison with the MoD. In

[67] CPNI, 'Who we work with'.
[68] CPNI, 'Who we work with'.
[69] CPNI, 'Who we work with'.
[70] Cabinet Office, *The UK Cyber Security Strategy*, p. 14.
[71] 'Chancellor's speech to GCHQ on cyber security'.
[72] CPNI, 'Who we work with'.
[73] MoD, *Cyber primer*, p. 1-20.
[74] MoD, *Cyber primer*, p. 1-20.

addition, there is a series of CERTs operating for national governments, universities and within industry—several of which are members of the global, but limited, Forum for Incident Response and Security Teams (FIRST).[75]

The reasons for attacks on CNI are multifarious; Verizon's 2014 Data Breach Investigations Report lists among them the longstanding problem posed by espionage.[76] This encompasses espionage by states as well as from private companies. The national interest remains dominant in conceptualizing cyber threats, but as we all swim in the same information ocean this does not deal sufficiently either with organized crime, which spans national jurisdictions (including those outside the EU and North America), or with building trust between states and state organizations. This need for 'building blocks' at the diplomatic level to establish 'red lines' and rules for state behaviour in cyberspace was an issue publicly raised by Richard Ledgett in the October 2015 interview he gave to the BBC.[77] In the same month, the Director-General of MI5, Andrew Parker, argued that the threat from terrorism stood at its highest level in his 32 years in the service, and that there were good reasons to increase international state-level collaboration.[78]

This call for increased state-based collaboration was subsequently incorporated into the 2015 SDSR, with responsible state-based behaviour in cyberspace championed by the 'London Cyber Process', which also paid heed to the challenges facing the current international economic and political order, identified as being 'driven by developments such as the growing role of non-state actors, the impact of technology and longer-term shifts of economic wealth to the south and east of the world'.[79]

For the UK, as a global financial and commercial hub, increased transparency, trust, and cooperation are also important for trade relations.[80] This realm encompasses the series of agreements, to a value of £30 billion, into which Britain has entered with China (including deals on the UK's next generation of civil nuclear power plants), and which raised concerns that these might provide gateways into strategic influence over computer-controlled UK CNI.[81] With China and Russia's intelligence agencies both accused of mapping the electricity grids in the United States and installing software traps which could be used to damage or disrupt their CNI, this concern cannot be easily dismissed, despite Chinese assurances.[82] These concerns are sufficient for the new UK Prime Minister, Theresa May, to delay these civil nuclear deals with China while the government re-examines them.[83]

[75] https://www.first.org/; see also MoD, *Cyber primer*, p. 1-20.
[76] Verizon Data Breach Investigations Report 2014.
[77] Corera, 'NSA warns of growing danger of cyber-attack by nation states'.
[78] 'MI5 boss wants "mature debate" on surveillance powers', BBC News, 29 Oct. 2015, http://www.bbc.co.uk/news/uk-34663929.
[79] HM Government, *National Security Strategy and Strategic Defence and Security Review 2015*, pp. 20, 41.
[80] HM Government, *National Security Strategy and Strategic Defence and Security Review 2015*, p. 17.
[81] 'Hammond rejects security fears over China investment', BBC News, 20 Oct. 2015, http://www.bbc.co.uk/news/uk-politics-34582673.
[82] Siobhan Gorman, 'Electricity grid in US penetrated by spies', *Wall Street Journal*, 8 April 2009, http://www.wsj.com/articles/SB123914805204099085; Kamal Ahmed, 'China admits—our reputation is on the line over nuclear security', BBC News, 21 Oct. 2015, http://www.bbc.co.uk/news/business-34595677. See also Alexander J. Martin, 'UK/China cyber security deal: national security attacks still OK, it seems', *The Register*, 22 Oct. 2015, http://www.theregister.co.uk/2015/10/22/uk_china_cyber_security_agreement_ip/.
[83] Carrie Grace, 'Hinkley Point: Theresa May's China calculus', BBC News, http://www.bbc.co.uk/news/

UK intelligence organizations

As outlined above, part of the protective barrier for CNI comes in the form of data collection by the UK's intelligence agencies: these comprise the Security Service (MI5), the Secret Intelligence Service (SIS/MI6) and GCHQ, with SIS and GCHQ reporting to the Foreign Secretary.[84] MI5 is primarily responsible for combating domestic and international terrorism and for counter-espionage, counter-proliferation and protective security and reports to the Home Secretary but it is not part of the Home Office.[85] The mainstay of MI6's remit is to collect secret intelligence and mount 'covert operations overseas in support of British Government objectives' relating to British foreign and defence policy, the UK's economic well-being, and the prevention and detection of serious crime.[86]

As Alex Younger, the current head of MI6, warned in March 2015: 'Using data appropriately and proportionately offers us a priceless opportunity to be even more deliberate and targeted in what we do and thus be better at protecting our agents and this country.' He went on to caution: 'That is good news. The bad news is that the same technology in opposition hands, an opposition often unconstrained by consideration of ethics and law, allows them to see what we are doing and put our people and agents at risk.'[87]

Within GCHQ, whose 'primary customers are the MOD, Foreign and Commonwealth Office and law enforcement agencies',[88] the main arm for dealing with threats to CNI is CESG. CESG acts as the 'National Technical Authority for Information Assurance within the UK' through three sets of interrelated activities 'in partnership with industry and academia' alongside their partner agencies, CPNI, MI5 and SIS/MI6.[89] These three activities are:

- guidance and tailored advice to UK government and the critical national infrastructure on the security risks of new and existing IT systems, providing ideas, designs and consultancy to protect against these risks;
- ensure appropriately assured products, services and people are available;
- deliver operational support to existing systems by alerting to specific threats and vulnerabilities, and provide incident response and technical solutions (such as cryptographic keys) to protect the most sensitive information.[90]

CESG also supports the British government by 'protecting sensitive material from hostile threats', ensuring 'capability and capacity needed to manage cyber security risks', 'securing Government interactions online with citizens', and 'advice on

world-36937511, 31 July 2016

[84] MoD, *Cyber primer*, p. 1-17. See also 'Intelligence and Security Act (ISA) section 7', 24 July 2016, http://intelligencecommissioner.com/content.asp?id=24#.

[85] MI5, 'What we do'.

[86] https://www.sis.gov.uk/our-mission.html, accessed 18 March 2015.

[87] Gordon Corera, 'Plaque unveiled for first MI6 chief Mansfield Cumming', BBC News, 31 March 2015, http://www.bbc.co.uk/news/uk-32126061.

[88] MoD, *Cyber primer*, p. 1-17.

[89] 'CESG: the Information Security Arm of GCHQ', https://www.cesg.gov.uk/articles/cesg-information-security-arm-gchq, accessed 26 July 2016.

[90] 'CESG: the Information Security Arm of GCHQ'.

Information Assurance Architecture and cyber security to UK government, critical national infrastructure, the wider public sector and suppliers to UK government'.[91]

In addition, there is JTAC, which analyses and assesses all-source intelligence relating to domestic and international terrorism. JTAC 'sets threat levels and issues warnings of threats and other terrorist-related subjects for customers from a wide range of government departments and agencies, as well as producing more in-depth reports on trends, terrorist networks and capabilities'. It functions as a 'self-standing organization comprised of representatives from sixteen government departments and agencies'.[92]

The 2015 SDSR increased funding for the security and intelligence services by £2.5 billion, half of which was dedicated to counterterrorism. This budget will permit the recruitment of 1,900 additional staff across the agencies described above to 'respond to, and deter those behind, the increasing international terrorist, cyber and other global threats', by means including offensive cyber capabilities.[93] The bulk of this funding is expected to go to GCHQ, which remains the dominant agency for UK cyber security.[94]

Within this framework can be discerned part of the rationale for UK participation in the PRISM mass surveillance programme.[95] That rationale is also reflected in the National Security Strategy and in the MoD's *Cyber primer* document, which states:

> The National Cyber Security Strategy seeks to secure the advantage in cyberspace by exploiting opportunities to gather intelligence and intervening as necessary against adversaries. Commanders should consider cyberspace to be an area of intelligence collection and analysis in its own right. Intelligence support to operations within cyberspace is essential to provide knowledge, reduce uncertainty, and support effective operational decision-making in defending MOD networks. It ... will include providing timely indicators and warnings ... [and] focuses on developing sound situational awareness and understanding by identifying trends and scanning for emerging threats, hazards or opportunities as well as understanding the consequences of any action. Cyberspace contains huge amounts of data which can be exploited and assessed for intelligence and situational awareness.

Furthermore:

> When observing changes in cyberspace, timescales vary from days or months to milliseconds. Individuals and groups operating in cyberspace leave digital trails but these can be disguised, thus making accurate identification, geo-location and attribution difficult. Exploiting this data-rich environment requires thorough intelligence preparation of the battlespace (IPB). Cyberspace has three interdependent layers which align with, and span, the physical, virtual and cognitive domains.[96]

[91] 'CESG: the Information Security Arm of GCHQ'.
[92] 'Joint Terrorism Analysis Centre', https://www.mi5.gov.uk/joint-terrorism-analysis-centre, accessed 31 March 2015.
[93] HM Government, *National Security Strategy and Strategic Defence and Security Review 2015*, p. 24.
[94] HM Government, *National Security Strategy and Strategic Defence and Security Review 2015*, p. 40; Lawson, 'The Joint Forces Command and the 2015 SDSR'.
[95] Luke Harding, *The Snowden files: the inside story of the world's most wanted man* (London: Guardian Books, 2014), pp. 155–69, 314–15, 323–8, and Glenn Greenwald, *No place to hide: Edward Snowden, the NSA, and the surveillance state* (London: Hamish Hamilton, 2014).
[96] MoD, *Cyber primer*, pp. 1-25–1-26.

The MoD also noted that:

While there are no international treaties specifically governing cyber activity, cyber operations must be conducted in accordance with existing domestic law. The international law that applies to military cyber operations will depend on whether an armed conflict is in existence, be it an international armed conflict or a non-international armed conflict. Where there is no armed conflict, military cyber activities are governed by domestic and international law applicable in peacetime.[97]

Relevant domestic legislation includes the Computer Misuse Act 1990,[98] the Data Retention and Investigatory Powers Act 2014[99] and the controversial Regulation of Investigatory Powers Act (RIPA) 2000,[100] as well as the equally controversial Draft Communications Data Bill (colloquially dubbed the 'Snooper's Charter').[101] International law includes the Law of Armed Conflict (LOAC) which adds both context and complexity to conflict in cyberspace. As the *Cyber primer* argues, this includes:

the prohibition on perfidy (inviting the confidence of an adversary as to protection under LOAC) and principles of neutrality. If the UK is the subject of an imminent or actual cyber attack that crosses the threshold so as to be an 'armed attack' as recognised by Article 51 of the UN Charter, the UK would be entitled to use force in national self-defence … Any response under self-defence must be necessary and proportionate. There is no consensus as to what degree of force constitutes an armed attack, other than that it must be an act/acts of armed force of sufficient gravity, having regard to its/their scale and effects.[102]

In addition, the implications of the law of self-defence turn on three practical issues: attribution; the speed with which an attack can be conducted, which can greatly reduce the ability to respond to an imminent attack; and the difficulty of determining intent, even if actions are provable and actors identifiable. Other difficulties posed by cyber events include deciding what is a lawful response to a (potentially hostile) cyber incident that may or may not cross the armed attack threshold.[103] This calculation, which has to be backed by legal opinion, is complicated by the 'attribution problem'. Such an incident could be generated by a state; a state-based actor; a private-sector company engaged in espionage; a group of individuals involved in cybercrime, or a state sponsoring it for its own ends (including for terrorist purposes); or an individual—whose reasons might range from malicious activity to curiosity. It is worth noting there have been cases of each.[104]

[97] MoD, *Cyber primer*, pp. 1-23–1-24.
[98] http://www.legislation.gov.uk/ukpga/1990/18/contents.
[99] http://www.legislation.gov.uk/ukpga/2014/27/contents/enacted. See also Jemima Kiss, 'Academics: UK "Drip" data law changes are "serious expansion of surveillance"', *Guardian*, 15 July 2014, http://www.theguardian.com/technology/2014/jul/15/academics-uk-data-law-surveillance-bill-rushed-parliament.
[100] http://www.legislation.gov.uk/ukpga/2000/23/contents. For countervailing views, see Big Brother Watch, http://www.bigbrotherwatch.org.uk/. See also David Anderson QC, 'Independent review of terrorist legislation', https://terrorismlegislationreviewer.independent.gov.uk/.
[101] http://www.parliament.uk/draft-communications-bill/.
[102] MoD, *Cyber primer*, p. 1-24.
[103] MoD, *Cyber primer*, p. 1-24.
[104] On cybercrime, see Misha Glenny, *Dark market: cyberthieves, cybercops and you* (London: Bodley Head, 2001), and *Dark market: how hackers became the new Mafia*.

Although advances in computer forensics mean that the attribution problem is decreasing there have also been cases where it is problematic (often deeply problematic from a legal standpoint) to identify the perpetrator.[105] This form of the 'attribution problem' leads to particular difficulties when the incident is a 'nation-state like attack', as it is known in the cyber-security community.[106] The attribution problem is already well recognized, and although a number of individuals have faced prosecution, many escape judicial proceedings (and it is quite likely that private-sector intrusions go undetected). Whether acts such as an attack on CNI committed by a cyber 'gun for hire' through the 'Dark Net' can be deterred or prosecuted is a major problem. By such means both states and non-state actors such as Al-Qaeda or Islamic State in Iraq and Syria (ISIS) can have a force multiplier effect on states hostile to them and become 'David' to 'Goliath'.[107] The possibility that ISIS and other hostile terrorist groups, as well as nation-states, might attack CNI was part of the reason why the SDSR increased the budgets for the security and intelligence agencies. In a speech at GCHQ in November 2015, George Osborne stated:

> ISIL [ISIS] are already using the internet for hideous propaganda purposes; for radicalisation, for operational planning too. They have not been able to use it to kill people yet by attacking our infrastructure through cyber attack. They do not yet have that capability. But we know they want it, and are doing their best to build it. So when we talk about tackling ISIL, that means tackling their cyber threat as well as the threat of their guns, bombs and knives. It is one of the many cyber threats we are working to defeat.[108]

In that same speech Osborne unequivocally stated: 'GCHQ is rightly known as equal to the best in the world. And I am clear that the answer to the question "who does cyber?" for the British government is—to very large degree—GCHQ.'[109]

Risk/resilience and UK 'governance' of CNI and devolved powers

Cyber security, which formerly fell within the purview of the Home Office, has since 2011 been overseen by the Cabinet Office, with scrutiny and political authority provided by the NSC. However, the picture is complicated by the fact that authority in some areas, including education and health, is now devolved to the Scottish Parliament, Northern Ireland Assembly and Welsh Government.[110] The political and social debates regarding the extent of devolution continue to evolve and are especially active in Scotland, which in September 2014 voted no in a

[105] Allan Cook, Andrew Nicholson, Helge Janicke, Leandros Maglaras and Richard Smith, 'Attribution of cyber attacks on industrial control systems', *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems* 3: 7, April 2016, pp. 1–15.
[106] See e.g. Rid, *Cyber war will not take place*, pp. 139–62.
[107] See e.g. Betz and Stevens, *Cyberspace and the state*, pp. 134–9; Jason Rivera, 'Achieving cyberdeterrence and the ability of small states to hold large states at risk', in Maybaum et al., eds, *2015 7th International Conference on Cyber Conflict*, pp. 7–24.
[108] 'Chancellor's speech to GCHQ on cyber security'.
[109] 'Chancellor's speech to GCHQ on cyber security'.
[110] 'Devolution: a beginner's guide', BBC Election 2010, 29 April 2010, http://news.bbc.co.uk/1/hi/uk_politics/election_2010/first_time_voter/8589835.stm.

referendum on full independence tabled by the ruling Scottish National Party, and where a second referendum cannot be ruled out. These constitutional arrangements naturally affect the governance of CNI in the UK as a whole, and will affect it further if more devolved powers or full independence (in the case of Scotland) are ceded by Westminster. The so-called 'West Lothian Question', whereby issues pertaining to only a part of the union—especially issues affecting only England—are voted on by all Westminster MPs, also bears on issues of governance of CNI.[111]

It is clear from the lists of devolved and non-devolved powers that while defence and national security remain under the control of Westminster, Scotland already has power for health, policing, the fire service and elements of transport; Northern Ireland for health and policing; and Wales for health, fire and rescue, and highways and transport. As noted above, each of these areas represents elements of CNI as defined by CPNI. It is important that cross-border collaboration for cyber resilience is clear and mutually reinforcing, because Britain is a relatively small land mass and what might appear to be a local incident could well disrupt or cascade to other areas.

Moreover, as the 2010 *Strategic framework and policy statement on improving the resilience of critical infrastructure to disruption from natural hazards* noted: 'There are some cross-sector themes such as technology wherein there may be infrastructure which supports the delivery of essential services across a number of sectors.'[112] CPNI, which also supports Britain's counterterrorism strategy (CONTEST), explains:

> This categorisation is done using the Government 'Criticality Scale', which assigns categories for different degrees of severity of impact. Not everything within a national infrastructure sector is 'critical'. Within the sectors there are certain 'critical' elements of infrastructure … The Criticality Scale includes three impact dimensions: impact on delivery of the nation's essential services; economic impact (arising from loss of essential service) and impact on life (arising from loss of essential service).[113]

As Philip Hammond, the then Defence Secretary, told the Defence Select Committee in October 2013, CPNI is

> where the impacts of cyber issues and cyber attacks on the broader national infrastructure are worked through, so that the vulnerabilities of utilities and other services that might be impacted by an attack on critical networks can be worked through and defensive strategies put in place. We have a number of mechanisms across Government that can absorb developments in one area and translate them into potential effects in other areas.[114]

Food and water are elements of national infrastructure (including some aspects clearly judged to be critical); these are among the areas devolved to the regional assemblies. Furthermore, central and local government is but one layer of 'gover-

[111] Duncan McTavish, 'Debate: Scotland, the United Kingdom and complex government', *Public Money and Management* 34: 1, 2014, pp. 4–8. See also Alexander Nicoll, 'Britain's integration debates', *Survival* 56: 6, 2014, pp. 209–18; Andrew M. Dorman, 'More than a storm in a teacup: the defence and security implications of Scottish independence', *International Affairs* 90: 3, May 2014, pp. 679–96.

[112] Cabinet Office, *Strategic framework*, p. 8.

[113] CPNI, 'The national infrastructure', http://www.cpni.gov.uk/about/cni/.

[114] House of Commons Defence Committee, *Towards the next Defence and Security Review: Part One*, 7th Report of Session 2013–14, vol. I (London, 18 Dec. 2013), http://www.publications.parliament.uk/pa/cm201314/cmselect/cmdfence/197/197.pdf.

nance'; private industry arguably has as great a (or a greater) say over the rules, regulation and governance of each of these sectors—a number of which will, at some level, be integrated with one another.[115] Clearly, there is a 'patchwork quilt' of responsibilities for CNI in these sectors and regions. The picture is complicated further by the fact that local councils, water boards and health-care trusts have their own sets of responsibilities and reporting mechanisms, while in some areas the private sector is dominant: these include communications, energy, financial services, food and transport.

For CNI protection in the event of natural disasters, there already exists a framework established following the Pitt Review conducted in the wake of the UK floods of 2007. The Pitt Review highlighted a number of resilience measures, among them:

- careful assessments of vulnerability, and prudent and proportionate risk mitigation activity, based on new, centrally defined standards;
- a shared framework to support cross-sector activity to assess, enhance and sustain the resilience of critical infrastructure and essential services to disruption;
- enhancing the collective capacity of critical infrastructure to absorb shock and act quickly when faced with unexpected events;
- effective emergency responses at the local level through improved information-sharing and engagement before, during and after emergencies.

These could equally apply to cyber resilience and help 'ensure that the Government, regulators, public sector bodies and owners of critical infrastructure are aware of the risks arising from … hazards and take appropriate action'.[116] This awareness encompasses the impact on society and the economy, which again can be analysed through a set of principles defined by the Pitt Review. These include:

1) a risk-based approach proportionate to the risks involved;
2) assessments of the likelihood and the consequences of critical infrastructure and essential services being severely disrupted, used to define standards and to set priorities;
3) calibration of the scale and cost of proposed programmes of measures to enhance resilience within each sector proportionate to the risks they face, including the 'criticality' of the infrastructure in question and its vulnerabilities, and the different options available to improve resilience;
4) cooperation and coordination within and between sectors and essential services, based on collaboration with the regional administrations on devolved matters to harmonize work programmes where possible to ensure appropriate standards for resilience are maintained across the UK;
5) planning to clarify the differences between sectors that arise from their different needs, circumstances and regulations with a view to building a National Resilience Plan for Infrastructure.

[115] For more on the issues of public–private partnerships see Madeline Carr, 'Public–private partnerships in national cyber-security strategies', *International Affairs* 92: 1, Jan. 2016, pp. 43–62.
[116] Cabinet Office, *Strategic framework*, p. 9.

In practice this means government departments will continue to sponsor and take the lead for their sectors, and to share information on dependencies, interdependencies and arrangements for business continuity management across sectors. This instils a precautionary approach to the uncertainties in the estimation of the risks posed covering all nine sectors of national infrastructure while recognizing that each sector is at a different starting point in establishing expectations and common goals. The sponsoring departments are responsible for deciding upon the appropriate security approach to be taken for their respective sectors. This means that analysis can be developed, and supporting evidence gathered, through formal and informal consultation to enable the development of sector resilience plans. This work should be coordinated with the CPNI and could be placed within the National Risk Register (NRR) or be made a subset of it.

Some elements of these proposals are likely to fall under the Civil Contingencies Act 2004, and would be subject to ministerial approval as well as parliamentary/regional scrutiny. This could be accomplished via national multisector strategic coordination and planning groups for national infrastructure, such as can already, in principle, be provided by CPNI/OCSIA and overseen by the NCSC. This could help coordinate top-down government action and bottom-up resilience and recovery. In addition a National Asset Database, similar to that operating in the US and used as a 'single classified prioritized list of [critical] systems and assets', should be developed if it is not already.[117]

As mentioned in the Pitt Review principles, the development of sector resilience plans could better enable 'Government and industry working together to foster a collective responsibility for enhancing resilience'.[118] The Pitt Review proposed that these plans be 'developed jointly through a tripartite relationship between the relevant government department, economic regulator and industry sector', and that they 'should be public documents with controlled sections where necessary for sensitive information'.[119] The Pitt Review also recommended that:

> Responsibility for producing the Plans will rest with the lead government department for each sector, with information provided by owners of critical infrastructure within the sector. Sector Resilience Plans are reviewed in an agreed timeframe. The programme will review existing regulation and guidance, identifying best practice and existing gaps in provision. It will also review current affordability appraisal practices in each sector, addressing how any improvements can be funded and whether any legal powers are needed to improve resilience.[120]

Adopting this approach, which has both regional and national applications and implications, would foster periodic bottom-up risk assessments and analysis.

[117] http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title6-section124l&num=0&edition=prelim, accessed 3 Aug. 2016

[118] 'Learning the lessons from the 2007 floods: an independent review by Sir Michael Pitt', June 2008, p. 242, http://webarchive.nationalarchives.gov.uk/20100807034701/http://archive.cabinetoffice.gov.uk/pittreview/_/media/assets/www.cabinetoffice.gov.uk/flooding_review/pitt_review_full%20pdf.pdf, accessed 26 July 2016.

[119] Cabinet Office, *Strategic framework*.

[120] Cabinet Office, *Strategic framework*.

The Criticality Scale

The Criticality Scale, on which CPNI draws, utilizes 'a co-ordinated approach to driving up the resilience of critical infrastructure' while the Cabinet Office noted the 'gap in the Government's policy-making and delivery towards the protection of critical infrastructure from severe disruption caused by natural hazards'.[121] The Criticality Scale is also useful for mapping the environment as it relates to cyber security, as can be seen in table 1.

Table 1: The Criticality Scale for national infrastructure

Criticality Scale category	*Description*
CAT 5	This is infrastructure the loss of which would have a catastrophic impact on the UK. These assets will be of unique national importance whose loss would have national long-term effects and may impact across a number of sectors. Relatively few are expected to meet the Cat 5 criteria.
CAT 4	Infrastructure of the highest importance to the sectors should fall within this category. The impact of loss of these assets on essential services would be severe and may impact provision of essential services across the UK or to millions of citizens.
CAT 3	Infrastructure of substantial importance to the sectors and the delivery of essential services, the loss of which could affect a large geographic region or many hundreds of thousands of people.
CAT 2	Infrastructure whose loss would have a significant impact on the delivery of essential services leading to loss, or disruption, of service to tens of thousands of people or affecting whole counties or equivalents.
CAT 1	Infrastructure whose loss could cause moderate disruption to service delivery, most likely on a localized basis and affecting thousands of citizens.
CAT 0	Infrastructure the impact of the loss of which would be minor (on a national scale).

Source: Strategic framework and policy statement on improving the resilience of critical infrastructure to disruption from natural hazards, March 2010.

In terms of mitigating risk and enhancing resilience, this provides a useful framework upon which CPNI can draw to map existing and future vulnerabilities and to examine in detail the sectors concerned. This examination should go

[121] Cabinet Office, *Strategic framework*.

much further than a dialogue with private industry and sharing of information on a voluntary basis; it should ideally be enshrined in law along the lines of US legislation and practices, as well as good practices found in Germany and Estonia, and the principles of the EU's NIS Directive should be embraced (as they will have no legal standing in the UK after Brexit). These approaches are not an end in themselves.[122] Dialogue and information-sharing on threats and vulnerabilities are a good starting point but do not go far enough.

Private industry, as the owner–operators of the vast majority of CNI, alongside the hardware and software companies upon which they rely for the maintenance of their systems, needs to feel confident in the government's ability to help them manage and mitigate these threats. In turn this would give the government greater confidence that they have grasped the national CNI environment and have a clear view of the landscape. It is not helpful to hold the view that 'the owners of Critical National Infrastructure need to be held to account'.[123] It is equally alarming that risks for the private sector are growing faster than their ability to act and governments are not seen to be doing enough. 'Risk tolerance' and risk awareness varies between businesses and sectors, while the British government is accused of being reluctant and too slow in sharing information/intelligence.[124] The revelations of the PRISM programme and the WikiLeaks disclosures of classified government information focused attention on the difficulties of where to draw the lines between 'the need to know' and 'the need to share' information/intelligence; and the balance between them needs to be better managed.[125]

What is required in practical terms is for government experts from the various bodies outlined above, especially those from the NCSC, OCSIA and CPNI, along with those of the NCA as the main police body overseeing cybercrime, to be invited into the relevant facilities for 'inside the fence' site assistance visits. There also needs to be transparent discussion of the strengths and weaknesses of cybersecurity practices within each site and company, from which best practices can be identified for each sector or nationwide. This set of best practices could function in a similar vein to the US Protected Critical Infrastructure Information (PCII) Program. The PCII is designed in a way that protects commercially sensitive or proprietary information and is used to analyse and secure critical infrastructure and protected systems; identify vulnerabilities and develop risk assessments; and enhance recovery preparedness measures. Adopting this approach through domestic legislation would permit the British government and its constituent elements to harden the protection of CNI from malicious attack.

[122] Kristan Stoddart, Kevin Jones, Hugh Soulsby, Andrew Blyth, Peter Eden, Peter Burnap and Yulia Cherdantseva, 'Live free or die hard: cybersecurity and government/corporate responses to threats to SCADA and industrial control systems in the US and UK', *Political Science Quarterly*, forthcoming 2016.

[123] Views expressed under the Chatham House rule at the 'National Security summit', London, 21 Oct. 2014.

[124] Views expressed under the Chatham House rule at the conference on 'Cyber security: building resilience reducing risk', London, Chatham House, 19–20 May 2014.

[125] On WikiLeaks, see David Leigh and Luke Harding, *WikiLeaks: inside Julian Assange's war on secrecy* (London: Guardian Books, 2011).

Government planning, private industry and owner–operators

This approach is not without its difficulties. Increased regulation, let alone new legislation, is likely to be resisted by private industry for a variety of longstanding reasons. The UK government, with or without EU or US support, is also unlikely to favour increased regulation or legislation which promotes state intervention—even for state-wide security reasons. Not only could this increase costs; there is also a legitimate question of where the expertise, as well as the money, will be found. It is also worth asking whether there is any political appetite for endeavours of this nature in the absence of a major cyber attack on the UK's CNI. Should such an event occur, however, the question would inevitably be asked: 'Could this have been prevented?' The answer to that question will depend on the nature and extent of the attack, the disruption or damage caused, any cascade effects, and the response and responsibility of private industry. The possibilities are not lost on the government. George Osborne stated at GCHQ in November 2015:

> If the lights go out, the banks stop working, the hospitals stop functioning or government itself can no longer operate, the impact on society could be catastrophic. So government has a responsibility towards these sectors, and the companies in those sectors have a responsibility to ensure their own resilience. Any new regulation will need to be carefully done—light enough and supple enough that it can keep up with the threat, so it encourages growth and innovation rather than suffocates it.[126]

The steps advocated in this article, alongside those contained in the 2015 SDSR, are designed to improve resilience to these threats in advance of any such attack. At the very least they will help both government and private industry to map domestic vulnerabilities, to assess what might be done to mitigate risk in a cost-effective manner and to keep a watching brief on areas of mutual concern. Should the kind of 'Cyber Pearl Harbor' or 'Cyber 9/11' event evoked by the former US Defense Secretary Leon Panetta actually materialize, the results could be potentially catastrophic. Such an attack could be directed at, for example:

- a chemical plant or refinery, leading to the release of toxic gases, oil or chemical spillages, or explosions;
- part of the UK traffic system: manipulation of the traffic light system in a major city alone could cause disruption or fatalities;
- dams, which regulate the water supply and provide electricity for large geographical areas; damage, destruction or disruption here could cause flooding, lead to a lack of clean drinking water and sanitation, disrupt navigation and transport, and have serious effects on industrial plants dependent on water (e.g. for cooling) and electricity supplies.[127]

[126] 'Chancellor's speech to GCHQ on cyber security'.

[127] These examples, like the others cited in this article, are grounded in real-world scenarios. See e.g. 'Iranian hackers "targeted" New York dam', BBC News, 21 Dec. 2015, http://www.bbc.co.uk/news/technology-35151492; Robert Lipovsky and Anton Cherepanov, 'BlackEnergy trojan strikes again: attacks Ukrainian electric power industry', *Welivesecurity*, 4 Jan. 2016, http://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/; Ian Hardy, 'Are smart city transport systems vulnerable to hackers?', BBC News, 5 Aug. 2016, http://www.bbc.co.uk/news/business-36854293.

An attack on any of these targets would place considerable strain on local and national response teams (including the emergency services and military). It would also place concomitant pressure on local and central government and agencies. The government, along with many others, is well aware of this. As the MoD's *Cyber primer* argues:

> Business continuity means being resilient and maintaining service while under attack. By developing a plan based on risk, resilience, impact and interdependency assessments, the effects of such an attack can be mitigated. Operators need to be made aware of which systems and, more importantly, what information/data is critical at which times during operations. When considering business continuity plans, the following should be considered.
>
> - Where does the priority lie in maintaining system availability?
> - What is the impact of system loss?
> - Who do I need to notify if I intend to close a system—or continue running it with known or even unknown faults?
> - How is risk measured and managed and at what levels of command do various responsibilities lie?
> - What is the recovery plan?
> - Is it frequently exercised using only back-up hardware, applications and data?[128]

While this is a useful series of questions to ask owner–operators in private industry, the UK government still needs to do much more to map and manage the vulnerabilities, mitigate major areas of risk, promote best practice through on-site inspections, and maintain a meaningful and transparent risk assessment process and risk register in a sustained partnership with private industry. Central government can help to coordinate the work of local government, government agencies, the police and emergency services and, if required, provide assistance or request help from its friends and allies—including NATO's CCDCOE. These measures will help to improve resilience before moving into the post-attack phase and, it is to be hoped, full recovery.

Conclusion and recommendations

With the rapid expansion of 'the Internet of Things', and moves within the UK and other developed and developing states towards 'smart' cities and 'smart' grids, the potential for malicious action will only rise. The MoD's *Cyber primer* states unequivocally: 'Cyberspace is contested even in peacetime—threat actors are constantly probing our networks seeking vulnerabilities, intelligence or military and commercial advantage.' It pertinently adds that 'civilian and military information infrastructures, whether national, coalition or international, co-exist and overlap, posing problems for managing security'.[129] For these reasons the UK government, as a responsible global actor, continues to promote 'responsible state

[128] MoD, *Cyber primer*, p. 1-30.
[129] MoD, *Cyber primer*, p. 1-23.

behaviour' in cyberspace.[130] However, this may not be enough. As Singer and Friedman argue: 'Cyber deterrence may play out on computer networks, but it's all about a state of mind.'[131] Jason Rivera also makes the case that 'cyberdeterrence strategy remains largely unexplored and underdeveloped, due to a limited understanding of how the principles of deterrence can be applied to the cyber domain'—with the added complexity posed by the attribution problem and legal restrictions.[132]

With this is mind, and despite the measures in place, it was noted in exchanges of the Defence Select Committee intended to inform the 2015 SDSR that scenarios for a major cyber attack on CNI are not practised by ministers or by the NSC.[133] This is a gap that can and should be addressed (for example, through the Cabinet Office Briefing Rooms). This would be especially valuable because the risk of escalation (intended or unintended) is high, and while governments are looking to private-sector actors to do more, private industry is also in the line of sight for hostile state actors.[134] Furthermore, the 2015 SDSR correctly noted that: 'Compromise or damage from these attacks may not be immediately visible.'[135] The SDSR also publicized the government's intention to work more closely with the owner–operators of CNI and drive up security across CNI, and announced the intention to 'establish a cyber training centre and test lab to support the development of more secure technology'.[136] Alongside this the government will practise 'new measures' against electrical power cuts and will review current measures for policing CNI with a view to building increased resilience and integration between sectors and organizations.[137] This is all positive and needs to be followed through in practice.

Currently, jurisdictional boundaries mean that many actors believe they can (and do) act with impunity. Responsible state behaviour means upholding the rule of law within and between states. Doing little or nothing about this at a global level ignores the fact that 'cyberspace does have a direct effect on the information environment … is very disruptive of many processes heretofore considered safe such as the exchange of money and the relative security of personal, industrial and governmental data, as we can see from the burgeoning statistics on cyber-crime and cyber-espionage'.[138]

The volume, types and complexity of cybercrime, cyber espionage, and the kinds of APTs now being seen pose a problem that is not going to change unless more robust measures are put in place. This means the UK, its allies and its friends need to develop coordinated information-sharing on a global scale and a series of

[130] Cabinet Office, *The UK Cyber Security Strategy*, p. 17.
[131] Peter W. Singer and Allan Friedman, *Cybersecurity and cyberwar: what everyone needs to know* (New York: Oxford University Press, 2014), p. 147.
[132] Rivera, 'Achieving cyberdeterrence', pp. 8–9.
[133] House of Commons Defence Committee, *Towards the next Defence and Security Review: Part One*, 7th Report of Session 2013–14, vol. I.
[134] Views expressed under the Chatham House rule at CyCon 2015.
[135] HM Government, *National Security Strategy and Strategic Defence and Security Review 2015*, p. 18.
[136] HM Government, *National Security Strategy and Strategic Defence and Security Review 2015*, p. 44.
[137] HM Government, *National Security Strategy and Strategic Defence and Security Review 2015*, p. 44.
[138] Betz and Stevens, *Cyberspace and the state*, p. 129.

state-based confidence-building measures rooted in international law. Prosecutions outside jurisdictional boundaries will need to be hammered out both bilaterally in test cases and multilaterally in environments such as the Internet Governance Forum (IGF). Attempts to impose state-based law and state-based regulation *must* take account of the views of the private sector, which is responsible for 80 per cent of the business that takes place online and provides most of the hardware and software underpinning the technology that enables the internet to function. Systemic resilience can only take root through a multi-stakeholder system that recognizes the limitations on the ability of nation-states to police the internet. While recognizing these limitations, this article has highlighted a number of steps that can be taken to better protect the UK's CNI from cyber threats, alongside the plans outlined in the 2015 SDSR.

In summary: the National Cyber Security Centre is a positive step if it fully engages all the relevant stakeholders within government and does not exclusively reflect the views of GCHQ or government. Engagement and partnership with the private sector, and the owner–operators of CNI, are vital to the success of the NCSC and the government's National Cyber Security Strategy. Legislating the reporting of cyber-security breaches to central government is essential for the protection of CNI. If problems remain hidden or unknown, this is a recipe for potential disaster. The Criticality Scale for natural disasters should be used as a measure of cyber resiliency and recommendations adapted from the 2007 Pitt Review should be implemented. Sector resilience plans should be adopted through CPNI and coordinated within the National Risk Register. A Protected Critical Infrastructure Information (PCII) Program should be adopted along US lines but tailored to the UK. Site assistance visits led by the NCSC should be promoted for CNI sites and the threat environment as it relates to CNI should be mapped. All this can only be accomplished with the full agreement of private industry as owner–operators. While the SDSR stated that 'the Government will avoid regulation wherever possible', this may not be a feasible approach if it is fully to protect the critical national infrastructure which underpins the British state.[139]

[139] HM Government, *National Security Strategy and Strategic Defence and Security Review 2015*, p. 73.